Polynomial functions of degree 20 which are APN infinitely often.

Florian Caullery
Institut of Mathematiques of Luminy
C.N.R.S.
France
florian.caullery@etu.univ-amu.fr

January 25, 2013

Abstract

We give all the polynomials functions of degree 20 which are APN over an infinity of field extensions and show they are all CCZ-equivalent to the function x^5, which is a new step in proving the conjecture of Aubry, McGuire and Rodier.

Keywords: vector Boolean functions, almost perfect nonlinear functions, algebraic surface, CCZ-equivalence.

1 Introduction

Modern private key crypto-systems, such as AES, are block cipher. The security of such systems relies on what is called the S-box. This is simply a Boolean function $f : \mathrm{F}_{2^n} \to \mathrm{F}_{2^n}$ where n is the size of the blocks. It is the only non linear operation in the algorithm.

One of the best known attack on these systems is differential cryptanalysis. Nyberg proved in [13] that the S-boxes with the best resistance to such attacks are the one who are said to be Almost Perfectly Non-linear (APN).

Let $q = 2^n$. A function $f : \mathrm{F}_q \to \mathrm{F}_q$ is said APN on F_q if the number of solutions in F_q of the equation

$$f(x + a) + f(x) = b$$

is at most 2 for all $a, b \in \mathrm{F}_q$, $a \neq 0$. The fact that F_q has characteristic 2 implies that the number of solutions is even for any function f on F_q.

The study of APN functions has focused on power functions and it was recently generalized to other functions, particularly polynomials (Carlet, Pott and al. [5, 7, 8]) or polynomials on small fields (Dillon [6]). On the other hand, several authors (Berger, Canteaut, Charpin, Laigle-Chapuy [2], Byrne, McGuire

[4] or Jedlicka [10]) showed that APN functions did not exist in certain cases. Some also studied the notion of being APN on other fields than F_{2^n} (Leducq [12]).

Toward a full classification of all APN functions, an approach is to show that certain polynomials are not APN for an infinity of extension of F_2.

Hernando and McGuire showed a result on classification of APN functions which was conjectured for 40 years : the only exponents such that the monomial x^d is APN over an infinity of extension of F_2 are of the form 2^i+1 or 4^i-2^i+1. Those exponents are called *exceptional exponents*.

It lead Aubry, McGuire and Rodier to formulate the following conjecture:

Conjecture: (Aubry, McGuire and Rodier) a polynomial can be APN for an infinity of ground fields F_q if and only if it is CCZ-equivalent (as defined by Carlet, Charpin and Zinoviev in [5]) to a monomial x^d where d is an exceptional exponent.

A way to prove this conjecture is to remark that being APN is equivalent to the fact that the rational points of a certain algebraic surface X in a 3-dimensional space linked to the polynomial f defining the Boolean function are all in a surface V made of 3 planes and independent of f. We define the surface X in the 3-dimensional affine space A^3 by

$$\phi(x,y,z)=\frac{f(x)+f(y)+f(z)+f(x+y+z)}{(x+y)(x+z)(y+z)}$$

which is a polynomial in $F_q[x,y,z]$. When the surface is irreducible or has an irreducible component defined over the field of definition of f, a Weil's type bound may be used to approximate the number of rational points of this surface. When it is too large it means the surface is too big to be contained in the surface V and the function f cannot be APN.

This way enabled Rodier to prove in [14] that when the degree of f is equal to $4e$ with $e \equiv 3 \pmod 4$ and ϕ is not divisible by a certain form of polynomial then f is not APN for an infinity of extension of F_q. He also found all the APN function of degree 12 and proved they are all CCZ-equivalent to x^3.

To continue in this way, let's get interested in the APN functions of degree 20 which were the next ones on the list. The main difference in this case is that $e \equiv 1 \pmod 4$. We got inspired by the proof of Rodier in [14] but we had an other approach using divisors of the surface $\bar{X}$. This was due to the fact that some of the components of $\bar{X}$ are no longer irreducible in our case.

Then we were able to obtain all the APN functions of degree 20 by calculation. The conditions of divisibility by the polynomials we obtained made the first part of our work, we had to work on the quotient after to obtain the final forms of the functions.

The second part was to prove that all were CCZ-equivalent to x^5.

This work has been done with François Rodier as adviser.

2 The state of the art

The best known APN functions are the Gold functions x^{2^i+1} and the Kasami-Welch functions by $x^{4^i-2^i+1}$. These 2 functions are defined over F_2 and they are APN on any field F_{2^m} if $\gcd(m,i)=1$. Aubry, McGuire and Rodier obtained the following results in [1].

Theorem 1 ***(Aubry, McGuire and Rodier, [1])*** *If the degree of the polynomial function f is odd and not an exceptional number then f is not APN over F_{q^n} for all n sufficiently large.*

Theorem 2 ***(Aubry, McGuire and Rodier [1])*** *If the degree of the polynomial function f is $2e$ with e odd and if f contains a term of odd degree, then f is not APN over F_{q^n} for all n sufficiently large.*

There are some results in the case of Gold degree $d=2^i+1$:

Theorem 3 ***(Aubry, McGuire and Rodier [1])*** *Suppose $f(x)=x^d+g(x)$ where $\deg(g)\leqslant 2^{i-1}+1$. Let $g(x)=\sum_{j=0}^{2^{i-1}+1} a_j x^j$. Suppose moreover that there exists a nonzero coefficient a_j of g such that $\phi_j(x,y,z)$ is absolutely irreducible (where $\phi_j(x,y,z)$ denote the polynomial $\phi(x,y,z)$ associated to x^j). Then f is not APN over F_{q^n} for all n sufficiently large.*

And for Kasami degree as well:

Theorem 4 ***(Férard, Oyono and Rodier [9])*** *Suppose $f(x)=x^d+g(x)$ where d is a Kasami exponent and $\deg(g)\leqslant 2^{2k-1}-2^{k-1}+1$. Let $g(x)=\sum_{j=0}^{2^{2k-1}-2^{k-1}+1} a_j x^j$. Suppose moreover that there exist a nonzero coefficient a_j of g such that $\phi_j(x,y,z)$ is absolutely irreducible. Then $\phi(x,y,z)$ is absolutely irreducible.*

Rodier proved the following results in [14]. We recall that for any function $f:\mathrm{F}_q\to\mathrm{F}_q$ we associate to f the polynomial $\phi(x,y,z)$ defined by:

$$\phi(x,y,z)=\frac{f(x)+f(y)+f(z)+f(x+y+z)}{(x+y)(x+z)(y+z)}.$$

Theorem 5 ***(Rodier [14])*** *If the degree of a polynomial function f is even such that $\deg(f)=4e$ with $e\equiv 3\pmod 4$, and if the polynomials of the form*

$$(x+y)(x+z)(y+z)+P,$$

with

$$P(x,y,z)=c_1\left(x^2+y^2+z^2\right)+c_4(xy+xz+zy)+b_1(x+y+z)+d,$$

for $c_1,c_4,b_1,d\in\mathrm{F}_{q^3}$, do not divide ϕ then f is APN over F_{q^n} for n large.

There are more precise results for polynomials of degree 12.

Theorem 6 ***(Rodier [14])*** *If the degree of the polynomial f defined over F_q is 12, then either f is not APN over F_{q^n} for large n or f is CCZ equivalent to the Gold function x^3.*

3 New Results

We have been interested in the functions defined by a polynomial of degree 20.

The main difference with the case already studied is that, when $e = 5$, $\phi_e(x, y, z)$ (where $\phi_e(x, y, z)$ denote the polynomial $\phi(x, y, z)$ associated to x^e) is not irreducible. So we had to detail more cases in the proof and use divisors on the surface X. And then obtained the following results :

Theorem 7 *If the degree of a polynomial function defined over F_q is 20 and if the polynomials of the form*

$$(x + y)(x + z)(y + z) + P_1$$

with $P_1 \in \mathrm{F}_{q^3}[x, y, z]$ and $P_1(x, y, z) = c_1(x^2 + y^2 + z^2) + c_4(xy + xz + yz) + b_1(x + y + z) + d$

or

$$\phi_5 + P_2$$

with $P_2 = a(x + y + z) + b$

do not divide ϕ then f is APN over F_{q^n} for n large.

Theorem 8 *If the degree of the polynomial f defined over F_q is 20, then either f is not APN over F_{q^n} for large n or f is CCZ equivalent to the Gold function x^5.*

4 Preliminaries

The following results are needed to prove the theorem 7 All the proofs are in [14].

Proposition 1 *[14]The class of APN functions is invariant by adding a q-affine polynomial.*

Proposition 2 *[14]The kernel of the map*

$$f \to \frac{f(x) + f(y) + f(z) + f(x + y + z)}{(x + y)(x + z)(y + z)}$$

is made of q-affine polynomials.

We define the surface X in the 3-dimensional affine space A^3 by

$$\phi(x, y, z) = \frac{f(x) + f(y) + f(z) + f(x + y + z)}{(x + y)(x + z)(y + z)}$$

and we call $\bar{X}$ its projective closure.

Proposition 3 *[14]If the surface X has an irreducible component defined over the field of definition of f which is not one of the planes $(x + y)(x + z)(y + z) = 0$, the function f cannot be APN for infinitely many extensions of F_q.*

Lemma 1 *[11]Let H be a projective hyper-surface. If $\bar{X} \cap H$ has a reduced absolutely irreducible component defined over F_q then $\bar{X}$ has an absolutely irreducible component defined over F_q.*

Lemma 2 *[1]Suppose d is even and write $d = 2^j e$ where e is odd. In $\bar{X} \cap H$ we have*

$$\phi_d = \phi_e\left(x, y, z\right)^{2^j} \left(\left(x+y\right)\left(x+z\right)\left(y+z\right)\right)^{2^j\text{-}1}$$

Lemma 3 *[14]The function $x+y$ (and therefore A) does not divide $\phi_i\left(x, y, z\right)$ for i an odd integer.*

Lemma 4 *ϕ_5 is not irreducible and we have*

$$\phi_5 = \left(x + \alpha y + \alpha^2 z\right)\left(x + \alpha^2 y + \alpha z\right)$$

with $\alpha \in \mathrm{F}_4$-F_2.

Calculus is sufficient to prove this.

5 Proof of theorem 7

Let $f : \mathrm{F}_q \rightarrow \mathrm{F}_q$ be a function which is APN over infinitely many extensions of F_q. As a consequence of proposition 11 no absolutely irreducible component of X is defined over F_q, except perhaps $x+y=0$, $x+z=0$ or $y+z=0$.

If some component of X is equal to one of these planes then by symmetry in x, y, and z, all of them are component of X, which implies that $A = \left(x+y\right)\left(x+z\right)\left(y+z\right)$ divides ϕ. Let us suppose from now on that this is not the case.

Let H_∞ is the plane at infinity of A^3 and $X_\infty = \bar{X} \cap H_\infty$. The equation of X_∞ is $\phi_{20} = 0$ which gives, using lemma 13 and 14

$$A^3 \left(x + \alpha y + \alpha^2 z\right)^4 \left(x + \alpha^2 y + \alpha z\right)^4 = 0$$

As the curve X_∞ does not contain any irreducible component defined over F_q, $\alpha \notin \mathrm{F}_q$ and then $q = 2^n$ with n odd.

Let X_0 be a reduced absolutely irreducible component of $\bar{X}$ which contains the line $x+y=0$ in H_∞. The cases where X_0 contains 2 or 3 copies of the line $x+y=0$ in H_∞ and where X_0 contains one copy of the line $x+y=0$ and is of degree 1 are treated in [14] and do not differ in our case. So from now on we assume that X_0 contains only one copy of the line $x+y=0$ and is at least of degree 2.

Let d_1 be the plane of equation $\left(x + \alpha y + \alpha^2 z\right) = 0$, d_2 the plane of equation $\left(x + \alpha^2 y + \alpha z\right) = 0$ we denote $C_i = d_i \cap H_\infty$ for $i = 1, 2$. Let A_0 be the line of equation $x+y=0$ in H_∞ , A_1 the line of equation $y+z=0$ in H_∞ and A_2 the line of equation $x+z=0$ in H_∞.

Let us consider D the divisor associated to the hyperplane section $\bar{X} \cap H_\infty$, so

$$D = 4C_1 + 4C_2 + 3A_0 + 3A_1 + 3A_2$$

We now denote $\mathfrak{X}_0$ the divisor associated to the hyperplane section of X_0 which is a sub-divisor of D of degree at least 2. We will denote $\mathfrak{X}_1$ the divisor obtained from $\mathfrak{X}_0$ by applying the permutation (x, y, z), $\mathfrak{X}_2$ the divisor obtained from $\mathfrak{X}_0$ by applying the permutation (x, z, y), $\mathfrak{X}_3$ the divisor obtained from $\mathfrak{X}_0$ by applying the transposition (x, y), $\mathfrak{X}_4$ the divisor obtained from $\mathfrak{X}_0$ by applying the transposition (x, z) and $\mathfrak{X}_5$ the divisor obtained from $\mathfrak{X}_0$ by applying the transposition (y, z). As $\phi(x, y, z)$ is symmetrical in x, y and z we know that $\mathfrak{X}_i$ is a subdivisor of D for $i = 1, \ldots, 5$. The cases where $\mathfrak{X}_0 \geqslant 2A_0$ or $\mathfrak{X}_0 = A_0$ are already treated in [14] so we have to study the cases below.

5.1 Case where $\mathfrak{X}_0$ is of degree 2.

i. If $\mathfrak{X}_0 = A_0 + A_1$ therefore from [14] 5.7 we have a contradiction with the fact that $\mathfrak{X}_0$ is at most of degree 2.

ii. If $\mathfrak{X}_0 = A_0 + C_i$, then $\mathfrak{X}_1 = A_1 + C_i$, $\mathfrak{X}_2 = A_2 + C_i$, $\mathfrak{X}_3 = A_0 + C_j$, $\mathfrak{X}_4 = A_1 + C_j$, $\mathfrak{X}_5 = A_2 + C_j$ with $j \neq i$. As seen in [14] the group $<\rho>= \mathrm{Gal}\left(\mathrm{F}_{q^3}/\mathrm{F}_q\right)$ acts on X_0 and as X_0 is not defined over F_q there exist sub-varieties X_6, X_7 and X_8 which have, respectively the associated divisor $\mathfrak{X}_6$, $\mathfrak{X}_7$ and $\mathfrak{X}_8$. We have $\mathfrak{X}_6 = A_0 + C_i$, $\mathfrak{X}_7 = A_1 + C_i$ and $\mathfrak{X}_8 = A_2 + C_i$. Finally we have $\sum \mathfrak{X}_i \geqslant D$ which is a contradiction.

5.2 Case where $\mathfrak{X}_0$ is of degree 3.

i. The case where $\mathfrak{X}_0 = A_0 + A_1 + A_2$ has already been treated in [14], this is the case where $A + P_1$ divides ϕ.

ii. If $\mathfrak{X}_0$ contains 2 of the A_i from [14] 5.7 it contains the 3 and it is the same case than previously.

iii. If $\mathfrak{X}_0 = A_0 + 2C_i$, then $\mathfrak{X}_1 = A_1 + 2C_i$ and $\mathfrak{X}_2 = A_2 + 2C_i$, in this case $\mathfrak{X}_0 + \mathfrak{X}_1 + \mathfrak{X}_2 \geqslant D$ which is a contradiction.

iv. If $\mathfrak{X}_0 = A_0 + C_1 + C_2$, then $\mathfrak{X}_1 = A_1 + C_1 + C_2$ and $\mathfrak{X}_2 = A_2 + C_1 + C_2$, $\mathfrak{X}_3 = A_0 + C_1 + C_2$, $\mathfrak{X}_4 = A_1 + C_1 + C_2$ and $\mathfrak{X}_5 = A_2 + C_1 + C_2$. Then $\sum \mathfrak{X}_i \geqslant D$ which is a contradiction.

5.3 Case where $\mathfrak{X}_0$ is of degree 4.

i. If $\mathfrak{X}_0 = A_0 + A_1 + A_2 + C_i$, then $\mathfrak{X}_1 = A_0 + A_1 + A_2 + C_i$, $\mathfrak{X}_2 = A_0 + A_1 + A_2 + C_i$, $\mathfrak{X}_3 = A_0 + A_1 + A_2 + C_j$, $\mathfrak{X}_4 = A_0 + A_1 + A_2 + C_j$ and $\mathfrak{X}_5 = A_0 + A_1 + A_2 + C_j$. Then $\sum \mathfrak{X}_i \geqslant D$ which is a contradiction.

ii. If $\mathfrak{X}_0$ contains 2 of the A_i from [14] 5.7 it contains the 3 and we are in the same case than in i).

iii. If $\mathfrak{X}_0 = A_0 + 3C_i$, then $\mathfrak{X}_1 = A_1 + 3C_i$ and $\mathfrak{X}_2 = A_2 + 3C_i$. Then $\sum \mathfrak{X}_i \geqslant D$ which is a contradiction.

iv. If $\mathfrak{X}_0 = A_0 + 2C_i + C_j$ then $\mathfrak{X}_1 = A_1 + 2C_i + C_j$ and $X_2 = A_2 + 2C_i + C_j$, with $j \neq i$. Then $\sum \mathfrak{X}_i \geqslant D$ which is a contradiction.

5.4 Case where $\mathfrak{X}_0$ is of degree 5.

i. If $X_0 = A_0 + 2(C_1 + C_2)$, then $\mathfrak{X}_1 = A_1 + 2(C_1 + C_2)$ and $\mathfrak{X}_2 = A_2 + 2(C_1 + C_2)$. Then $\sum \mathfrak{X}_i \geqslant D$ which is a contradiction.

ii. If $\mathfrak{X}_0 = A_0 + 3C_i + C_j$, $j \neq i$, $\mathfrak{X}_1 = A_1 + 3C_i + C_j$ and $\mathfrak{X}_2 = A_2 + 3C_i + C_j$. Then $\sum \mathfrak{X}_i \geqslant D$ which is a contradiction.

iii. If $\mathfrak{X}_0 = A_0 + 4C_i$, then $\mathfrak{X}_1 = A_1 + 4C_i$ then $\mathfrak{X}_0 + \mathfrak{X}_1 \geqslant D$ which is a contradiction.

iv. If $\mathfrak{X}_0$ contains 2 of the A_i from [14] 5.7 it contains the 3 and we will treat those cases in the following points.

v. If $\mathfrak{X}_0 = A_0 + A_1 + A_2 + 2C_i$ then $\mathfrak{X}_1 = A_0 + A_1 + A_2 + 2C_i$ and $\mathfrak{X}_2 = A_0 + A_1 + A_2 + 2C_i$. Then $\sum \mathfrak{X}_i \geqslant D$ which is a contradiction.

vi. The only case left is when $X_0 = A_0 + A_1 + A_2 + C_1 + C_2$. As seen in [14] the group $< \rho >= \mathrm{Gal}\left(\mathrm{F}_{q^3}/\mathrm{F}_q\right)$ acts on X_0 and as X_0 is not defined over F_q there exist sub-varieties X_6, X_7 and X_8 which have, respectively the associated divisor $\mathfrak{X}_6$, $\mathfrak{X}_7$ and $\mathfrak{X}_8$. We have $\mathfrak{X}_6 = A_0 + A_1 + A_2 + C_1 + C_2$, $\mathfrak{X}_7 = A_0 + A_1 + A_2 + C_1 + C_2$ and $\mathfrak{X}_8 = A_0 + A_1 + A_2 + C_1 + C_2$. It remains the sub-divisor $\mathfrak{X}_9 = C_1 + C_2$. Therefore $\sum \mathfrak{X}_i = D$ and the form of ϕ is :

$$\phi = (\phi_5 + R)(A\phi_5 + Q)(A\phi_5 + \rho(Q))\left(A\phi_5 + \rho^2(Q)\right)$$

with R a polynomial of degree 1 such as $\phi_5 + R$ is not irreducible, Q a polynomial of degree 4 and ρ the generator of $\mathrm{Gal}\left(\mathrm{F}_{q^3}/\mathrm{F}_q\right)$.

It is useless to consider the cases where X_0 is of degree more than 5 as we obtain 2 other divisors of the same degree from X_0 and D is of degree 17. Therefore it is sufficient to prove the theorem 7.

6 Proof of theorem 8

We have the two following cases to study:

6.1 Case where $A + P_1$ divides ϕ.

If P_1 divides ϕ then $(A + P_1)(A + \rho(P_1))\left(A + \rho^2(P_1)\right)$ divides ϕ too (see [14]. By calculus (see Appendix 1) we can state that:

- $P_1 = c_1\phi_5 + c_1^3$.
- The trace of c_1 in F_{q^3} is 0.

- $(A+P_1)(A+\rho(P_1))\left(A+\rho^2(P_1)\right)$ is the polynomial ϕ associated to $L(x)^3$ where $L(x)=x(x+c_1)(x+\rho(c_1))\left(x+\rho^2(c_1)\right)$.

- We have $f=L(x)^3\left(L(x)^2+a\right)+a_{16}x^{16}+a_8x^8+a_4x^4+a_2x^2+a_1x+a_0$ where $a,a_0,a_1,a_2,a_4,a_8,a_{16}\in \mathrm{F}_q$.

By proposition 9 f is equivalent to $L(x)^5+aL(x)^3$. As $\mathrm{tr}(c_1)=0$, $L(x)$ is a q-affine permutation hence f is CCZ-equivalent to x^5+ax^3.

By theorem 3 f cannot be APN over infinitely many extensions of F_q if $a\neq 0$. Hence $a=0$ and f is CCZ-equivalent to x^5, which is a gold function.

6.2 Case where P_2 divides ϕ.

If P_2 divides ϕ then, by calculus (see Appendix 2), we obtain that $f=\left(x^{20}+ax^{10}+bx^5\right)+a_{16}x^{16}+a_8x^8+a_4x^4+a_2x^2+a_1x+a_0$, where $a,b,a_0,a_1,a_2,a_4,a_8,a_{16}\in \mathrm{F}_q$. By proposition 9 f is equivalent to $\left(x^5+ax^2+bx\right)^4$. Therefore f can be written $f(x)=L\left(x^5\right)$ with $L(x)=x^4+ax^2+bx$ which is a permutation. Hence, f is CCZ-equivalent to x^5.

In conclusion, we proved that if $f(x)$ is a polynomial of F_q of degree 20 which is APN over infinitely many extensions of F_q, then $f(x)$ is CCZ-equivalent to x^5.

References

[1] Y.Aubry, G. McGuire, F. Rodier, A few more functions that are not APN infinitely often, Finite Fields : Theory and applications, Ninth International conference Finite Fields and Applications, McGu et al.editors, Contemporary Math. n°518, AMS, Providence (RI), USA, 2010, pp23-31.

[2] T. Berger, A. Canteaut, P. Charpin, Y. Laigle-Chapuy On almost perfect nonlinear functions over F_{2^n}. IEEE Trans. Inform. Theory 52 (2006), no. 9, 4160-4170.

[3] L. Budaghyan and C. Carlet and P. Felke and G. Leander An infinite class of quadratic APN functions which are not equivalent to power mappings, Cryptology ePrint Archive, n° 2005/359

[4] Byrne E. and McGuire G., On the Non-Existence of Quadratic APN and Crooked Functions on Finite Fields, prepublication. http://www.maths.may.ie/sta/gmg/APNniceWeilEBGMG.pdf.

[5] C. Carlet, P. Charpin and V. Zinoviev. Codes, bent functions and permutations suitable for DES-like crypto-systems. Designs, Codes and Cryptography, 15(2), pp. 125-156, 1998.

[6] J. Dillon, APN Polynomials: An Update. Fq9, International Conference on Finite Fields and their Applications July 2009

[7] Y. Edel, G. Kyureghyan and A. Pott. A new APN function which is not equivalent to a power mapping. IEEE Trans. Inform. Theory 52 (2006), no. 2, 744-747.

[8] Y. Edel, A. Pott. A new almost perfect nonlinear function which is not quadratic Adv. Math. Commun. 3 (2009), no. 1, 59-81.

[9] E. Ferard, R. Oyono and F. Rodier. Some more functions that are not APN infinitely often. The case of Gold and Kasami exponents.

[10] Jedlicka, D., APN monomials over GF(2n) for infinitely many n, Finite Fields Appl. 13 (2007), no. 4, 1006-1028

[11] G.Leander and F.Rodier Bounds on the degree of APN Polynomials. The case of $x^{-1}+g(x)$. Designs, Codes and cryptography. 0925-1022. 2009

[12] Leducq E. A proof of two conjectures on APN functions, eprint arXiv:1006.4026

[13] K. Nyberg, Differentially uniform mappings for cryptography, Advances in cryptology-Eurocrypt '93 (Lofthus, 1993), 55-64, Lecture Notes in Comput. Sci., VOl. 765, Springer, Berlin, 1994.

[14] F. Rodier, Functions of degree 4e that are not APN infinitely often. Cryptogr. Commun. 3 (2011), n°4, 227-240.

7 Appendix

In this part we give the details of the calculus we made in order to state the theorem 8 We just use the fact that P_1 or P_2 divides ϕ and it gives us conditions on the coefficients of P_1 or P_2 and ϕ. As ϕ is a symmetrical polynomial in x, y, z we can write it using symmetrical functions $s_1 = x+y+z$, $s_2 = xy+xz+yz$ and $s_3 = xyz$. We recall that ϕ_i is the polynomial ϕ associated to x^i and therefore $\phi(x, y, z)$ the polynomial associated to $f(x) = \sum_{i=0}^{d} a_i x^i$ can be written $\phi = \sum a_i \phi_i$. Denoting $p_i = x^i + y^i + z^i$, we have $p_i = s_1 p_{i-1} + s_2 p_{i-2} + s_3 p_{i-3}$. We remark that $\phi_i = \frac{p_i + s_1^i}{A}$ and that $A = s_1 s_2 + s_3$.

The calculus were made on the software Sage and you can find the sheet at the following adress: http://sagenb.org/home/pub/5035.

7.1 Case where $A + P_1$ divides ϕ.

We will write P for P_1 in this section in order to make the calculus more readable.

If $A + P$ divides ϕ then $(A+P)(A+\rho(P))\left(A+\rho^2(P)\right)$ is of degree 9 and divides ϕ too (see [14]). We write

$$(A+P)(A+\rho(P))\left(A+\rho^2(P)\right) = \sum_{i=0}^{9} P_i,$$

where P_i is the term of degree i of $(A+P)(A+\rho(P))\left(A+\rho^2(P)\right)$.

As $(A+P)(A+\rho(P))\left(A+\rho^2(P)\right)$ divides ϕ there exists a polynomial Q of degree 8 such as

$$\phi = (A+P)(A+\rho(P))\left(A+\rho^2(P)\right)Q$$

and we write

$$Q=\sum_{i=0}^{8} Q_i,$$

where Q_i is the term of degree i of Q.

7.1.1 Degree 17

We put $a_{20}=1$ and we have :

$$\phi_{20}=P_9Q_8.$$

As $P_9=A^3$ we have $Q_8=\phi_5^4$.

7.1.2 Degree 16.

We have

$$a_{19}\phi_{19}=P_9Q_7+P_8Q_8.$$

As $P_8=A^2(s_1^2\operatorname{tr}(c_1)+s_2\operatorname{tr}(c_4))$, where $\operatorname{tr}(c_i)$ is the trace of c_1, it gives us

$$a_{19}\phi_{19}=A^3Q_7+A^2\phi_5^4(s_1^2\operatorname{tr}(c_1)+s_2\operatorname{tr}(c_4)).$$

As ϕ_{19} is not divisible by A (by lemma 13) so $a_{19}=0$ and

$$AQ_7=\phi_5^4(s_1^2\operatorname{tr}(c_1)+s_2\operatorname{tr}(c_4)).$$

We know that A is prime with $s_1^2\operatorname{tr}(c_1)+s_2\operatorname{tr}(c_4)$ because $(x+y)$ does not divide this polynomial, and A does not divide either ϕ_5^4 which implies $Q_7=P_8=0$ and $\operatorname{tr}(c_1)=\operatorname{tr}(c_4)=a_{19}=0$.

7.1.3 Degree 15.

We have

$$a_{18}\phi_{18}=a_{18}(A\phi_9^2)=P_9Q_6+P_8Q_7+P_7Q_8.$$

Knowing that $P_8=Q_7=0$ we obtain

$$a_{18}(A\phi_9^2)=P_9Q_6+P_7Q_8=A^3Q_6+\phi_5^4P_7.$$

We also know that

$$\phi_5^4=\left(s_1^2+s_2\right)^4=s_1^8+s_2^4$$

and

$$P_7 = A\left(s_1^4 q_1(c_1) + s_2^2 q_1(c_4) + s_1^2 s_2 q_5(c_1, c_4)\right) + A^2 s_1 \operatorname{tr}(b_1)$$

denoting
$q_1(c_i) = c_i \rho(c_i) + c_i \rho^2(c_i) + \rho(c_i)\rho^2(c_i)$ and
$q_5(c_1, c_4) = c_1\left(\rho(c_4) + \rho^2(c_4)\right) + c_4\left(\rho(c_1) + \rho^2(c_1)\right) + \rho(c_1)\rho^2(c_4) + \rho(c_4)\rho^2(c_1)$.
So

$$a_{18}\phi_9^2 = A^2 Q_6 + \phi_5^4\left(s_1^4 q_1(c_1) + s_2^2 q_1(c_4) + s_1^2 s_2 q_5(c_1, c_4) + A s_1 \operatorname{tr}(b_1)\right),$$

hence A divide $a_{18}\phi_9^2 + \phi_5^4\left(s_1^4 q_1(c_1) + s_2^2 q_1(c_4) + s_1^2 s_2 q_5(c_1, c_4)\right)$. As $A = s_1 s_2 + s_3$ the polynomial $a_{18}\phi_9^2 + \phi_5^4\left(s_1^4 q_1(c_1) + s_2^2 q_1(c_4) + s_1^2 s_2 q_5(c_1, c_4)\right)$ cannot contain monomial in s_1^{12} or s_2^6, therefore $a_{18} = q_1(c_1) = q_1(c_4)$.

Then A divides $a_{18}\left(\phi_9^2 + \phi_5^6\right) + \phi_5^4 s_1^2 s_2 q_5(c_1, c_4)$. As $\phi_9^2 + \phi_5^6 = A^4$ and A does not divide ϕ_5^4 we have $q_5(c_1, c_4) = 0$. Replacing in the first equation we have

$$a_{18} A^4 = A^2 Q_6 + A\phi_5^4 s_1(\operatorname{tr}(b_1)).$$

So

$$a_{18} A^3 + A Q_6 = \phi_5^4 s_1(\operatorname{tr}(b_1)),$$

as A does not divide $\phi_5^4 s_1$, $\operatorname{tr}(b_1) = 0$ and $Q_6 = a_{18} A^2$.

7.1.4 Degree 14.

We first prove that $c_1 = c_4$.

We have

$$a_{17}\phi_{17} = P_9 Q_5 + \ldots + P_6 Q_8 = P_9 Q_5 + P_6 Q_8.$$

We know that

$$P_6 = A^2 N(d) + A\left(s_1^3 q_5(c_1, b_1) + s_1 s_2 q_5(c_1, b_1)\right) + s_1^6 N(c_1) + s_1^4 s_2 q_4(c_1, c_4) + s_1^2 s_2^2 q_4(c_4, c_1) + s_2^3 N(c_4)$$

where

$N(a) = a\rho(a)\rho^2(a)$which is the norm of$a$inF_q.$q_4(a,b) = a\rho(a)\rho^2(b) + a\rho(b)\rho^2(a) + b\rho(a)\rho^2(a)$.$q_5(a,b) = a(\rho(b)+\rho$

for all a, b in F_{q^3}.

We can write

$$P_6 = A^2 \operatorname{tr}(d) + A\left(s_1^3 q_5(c_1, b_1) + s_1 s_2 q_5(c_1, b_1)\right) + P_6^* \rho(P_6^*)\rho^2(P_6^*),$$

where $P_6^* = c_1 s_1^2 + c_4 s_2$. So we can deduce that

$$a_{17}\phi_{17} = A^3 Q_5 + \phi_5^4\left(A^2 \operatorname{tr}(d) + A\left(s_1^3 q_5(c_1, b_1) + s_1 s_2 q_5(c_1, b_1)\right) + P_6^* \rho(P_6^*)\rho^2(P_6^*)\right).$$

We now have A divides $a_{17}\phi_{17} + \phi_5^4 P_6^* \rho(P_6^*)\rho^2(P_6^*)$. In addition, denoting $s = x + y$,

$$(x+z)^2\phi_5 = (x+z)^4 + s(x^2 y + x^2 z + y z^2 + z^3) = (x+z)^4 + s R_1$$

and

$$(x+z)^2\phi_{17} = (x+z)^{16} + sR_2,$$

where R_1 is a polynomial of degree 3 and R_2 is a polynomial of degree 15. As $(x+z)^8 A = (x+z)^9 s(x+z+s)$ divides $a_{17}(x+z)^8\phi_{17} + P_6^*\rho(P_6^*)\rho^2(P_6^*)(x+z)^8\phi_5^4$ which is equal to

$$a_{17}(x+z)^6\left(x^{16}+z^{16}+sR_1\right) + P_6^*\rho(P_6^*)\rho^2(P_6^*)\left(x^4+z^4+sR_2\right). \qquad (1)$$

Therefore we have $P_6^* = c_1(s^2+z^2) + c_4(x^2+s(x+z)) = c_1z^2 + c_4x^2 + sR_3 = P_6^{**} + sR_3$.

As s divides (1) the constant term in s vanishes :

$$(x+z)^{16}\left(a_{17}(x+z)^6 + P_6^{**}\rho(P_6^{**})\rho^2(P_6^{**})\right) = 0,$$

then

$$a_{17}(x+z)^6 + P_6^{**}\rho(P_6^{**})\rho^2(P_6^{**}) = 0,$$

hence

$$a_{17}(x+z)^6 + (c_4x^2+c_1z^2)(\rho(c_4)x^2+\rho(c_1)z^2)(\rho^2(c_4)x^2+\rho^2(c_1)z^2) = 0,$$

so

$$a_{17}(x+z)^3 + (\sqrt{c_4}x+\sqrt{c_1}z)(\rho(\sqrt{c_4})x+\rho(\sqrt{c_1})z)(\rho^2(\sqrt{c_4})x+\rho^2(\sqrt{c_1})z) = 0.$$

The polynomial $x+z$ divides $(\sqrt{c_4}x+\sqrt{c_1}z)(\rho(\sqrt{c_4})x+\rho(\sqrt{c_1})z)(\rho^2(\sqrt{c_4})x+\rho^2(\sqrt{c_1})z)$ so it divides one component and then $c_1 = c_4$.

We now calculate P_6 and Q_5.

As $c_1 = c_4$ we have $P_6 = A^2\,\mathrm{tr}\,(d) + A\phi_5 s_1 q_5\,(c_1, b_1) + \phi_5^3 N\,(c_1)$, so from $a_{17}\phi_{17} = P_9Q_5 + P_6Q_8$ we can deduce that A divides $a_{17}\phi_{17} + q_3\,(c_1)\,\phi_5^7$. Hence the coefficient of the monomials s_1^{14} in $a_{17}\phi_{17} + N\,(c_1)\,\phi_5^7$, which is $a_{17} + N\,(c_1)$, must be equal to 0, so $a_{17} = N\,(c_1)$.

Remarking that $\phi_{17} + \phi_5^7 = A^2\phi_5\phi_9$ we have A divides $\phi_5 s_1 q_5\,(c_1, b_1)$. As $\phi_5 s_1$ is not divisible by A we have $q_5\,(c_1, b_1)$=0. So now we have

$$A^3Q_5 = A^2\phi_5^4\,\mathrm{tr}\,(d) + a_{17}A^2\phi_5\phi_9,$$

which gives

$$AQ_5 = \phi_5^4\,\mathrm{tr}\,(d) + a_{17}\phi_5\phi_9.$$

Using the same argument as precedent we have $\mathrm{tr}\,(d) = N\,(c_1)$ and then $Q_5 = a_{17}\frac{\phi_5\phi_9+\phi_5^4}{A^2} = a_{17}A^2\phi_5$ and $P_6 = a_{17}\left(A^2+\phi_5^3\right)$.

7.1.5 Degree 13

We use

$$\begin{aligned} 0 = a_{16}\phi_{16} &= P_9Q_4 + P_8Q_5 + P_7Q_6 + P_6Q_7 + P_5Q_8 \\ &= A^3Q_4 + a_{18}^2A^3\phi_5^2 + \phi_5^4P_5, \end{aligned}$$

with

$$P_5 = q_4(c_1, b_1)\left(s_1^5 + s_2^2s_1\right) + A\left(q_1(b_1)s_1^2 + q_5(c_1, d)\left(s_1^2 + s_2\right)\right).$$

As A^3 does not divide $P_5\phi_5^4$, so $P_5 = 0$ and $q_4(c_1, b_1) = q_1(b_1) = q_5(c_1, d) = 0$.
We deduce

$$Q_4 = a_{18}^2\phi_5^2.$$

7.1.6 Degree 12

We have

$$\begin{aligned} a_{15}\phi_{15} &= P_9Q_3 + P_8Q_4 + P_7Q_5 + P_6Q_6 + P_5Q_7 + P_4Q_8 \\ &= A^3Q_3 + a_{18}a_{17}A^2\phi_5^3 + a_{18}a_{17}A^2\left(A^2 + \phi_5^3\right) + P_4\phi_5^4, \end{aligned}$$

with

$$P_4 = q_4(b_1, c_1)(s_1^4 + s_1^2s_2) + q_4(c_1, d)(s_1^4 + s_2^2) + q_5(b_1, d)As_1 = H_4 + AG_4,$$

where $H_4 = q_4(b_1, c_1)(s_1^4 + s_1^2s_2) + q_4(c_1, d)(s_1^4 + s_2^2)$ and $G_4 = q_5(b_1, d)s_1$. So $A|H_4\phi_5^4 + a_{15}\phi_{15}$. As

$$H_4\phi_5^4 + a_{15}\phi_{15} = s_1^{12}\left(a_{15} + q_4(b_1, c_1) + q_4(c_1, d)\right) + s_1^{10}s_2q_4(b_1, c_1) + a_{15}s_1^9s_3 + s_1^8s_2^2\left(a_{15} + q_4(c1, d)\right) + s_1^4s_2^4\left(q_4(b_1, c_1\right.$$

the coefficients of s_1^{12} and s_2^6 must be 0 and so

$$a_{15} + q_4(b1, c1) + q_4(c1, d) = 0 \text{ and} a_{15} + q_4(c1, d) = 0 \,\text{so}\, q_4(b1, c1) = 0.$$

Replacing in the equation we now have

$$H_4\phi_5^4 + a_{15}\phi_{15} = a_{15}\left(s_1^9s_3 + s_1^4s_2^4 + s_1^3s_3^3 + s_1s_2^4s_3 + s_3^4\right) = a_{15}\left(\phi_{15} + \phi_5^6\right),$$

but A does not divide $\phi_{15} + \phi_5^6$ so $a_{15} = 0$ so $H_4 = 0$.

Hence

$$0 = A^3Q_3 + a_{18}a_{17}A^2\phi_5^3 + a_{18}a_{17}A^2\left(A^2 + \phi_5^3\right) + AG_4\phi_5^4.$$

So A divides G_4, but the degree of G_4 is less than or equal to 1 so $G_4 = 0$ it implies $q_5(b_1, d) = 0$ so $P_4 = 0$.

We conclude

$$Q_3 = a_{18}a_{17}A.$$

7.1.7 Degree 11.

We have

$$a_{14}\phi_{14} = P_9Q_2 + P_8Q_3 + P_7Q_4 + P_6Q_5 + P_5Q_6 + P_4Q_7 + P_3Q_8,$$

so

$$a_{14}A(\phi_5^4 + s_1^2s_3^2) = A^3Q_2 + a_{18}^3A\phi_5^4 + a_{17}^2A\phi_5\left(A^2 + \phi_5^3\right) + P_3\phi_5^4. (*)$$

So A divides P_3. But $P_3 = N(b_1)s_1^3 + q_6(c_1, b_1, d))s_1\phi_5 + q_1(d)A$ so $N(b_1) = q_6(c_1, b_1, d) = 0$ with

$$q_6(c_1, b_1, d) = b_1\rho(c_1)\rho^2(d)+b_1\rho(d)\rho^2(c_1)+c_1\rho(b_1)\rho^2(d)+c_1\rho(d)\rho^2(b_1)+d\rho(c_1)\rho^2(b_1)+d\rho(c_1)\rho^2(b_1).$$

As $N(b_1) = 0, b_1 = 0$.

When we replace in the equation $(*)$ we have

$$A^3(Q_2 + a_{17}^2\phi_5) = A\left(\phi_5^4\left(a_{14} + a_{18}^3 + a_{17}^2 + q_1(d)\right) + a_{14}s_1^2s_3^2\right),$$

so A divides $\phi_5^4\left(a_{14} + a_{18}^3 + a_{17}^2 + q_1(d)\right)+a_{14}s_1^2s_3^2 = (s_1^8+s_2^4)\left(a_{14} + a_{18}^3 + a_{17}^2 + q_1(d)\right)+ a_{14}s_1^2s_3^2$, then $a_{14} + a_{18}^3 + a_{17}^2 + q_1(d) = 0$, with the same argument as before on the coefficients of the monomials s_1^8 and s_2^4, therefore $a_{14} = 0$ because A does not divide $s_1^2s_3^2$.

We obtain

$$Q_2 = a_{17}^2\phi_5,$$

and

$$P_3 = (a_{17}^2 + a_{18}^3)A.$$

7.1.8 Degree 10.

We have

$$a_{13}\phi_{13} = P_9Q_1 + P_8Q_2 + P_7Q_3 + P_6Q_4 + P_5Q_5 + P_4Q_6 + P_3Q_7 + P_2Q_8$$

$$= A^3Q_1 + a_{17}a_{18}^2A^2\phi_5^2 + a_{17}a_{18}^2\phi_5^2\left(A^2 + \phi_5^3\right) + \phi_5^4\left(s_1^2q_4\left(d, c1\right) + s_2q_4\left(d, c1\right)\right),$$

so A divides $a_{13}\phi_{13}+\phi_5^5\left(a_{17}a_{18}^2 + q_4\left(d, c1\right)\right) = a_{13}\left(s_1^4s_3^2 + s_1^3s_2^2s_3 + s_1^2s_2s_3^2 + s_1s_3^3\right)+ \phi_5^5\left(a_{13} + a_{17}a_{18}^2 + q_4\left(d, c1\right)\right)$. with the same argument as before on the coefficients of the monomials s_1^8 and s_2^4 we have

$$a_{13} + a_{17}a_{18}^2 + q_4\left(d, c1\right) = 0.$$

in addition, A does not divide $s_1^4s_3^2 + s_1^3s_2^2s_3 + s_1^2s_2s_3^2 + s_1s_3^3$ so $a_{13} = 0$ and $q_4(d, c1) = a_{17}a_{18}^2$.

Now we have

$$AQ_1 = 0.$$

So $Q_1 = 0$ and $P_2 = a_{17}a_{18}^2\phi_5$.

7.1.9 Degree 9.

We have

$a_{12}\phi_{12} = P_9Q_0 + P_8Q_1 + P_7Q_2 + P_6Q_3 + P_5Q_4 + P_4Q_5 + P_3Q_6 + P_2Q_7 + P_1Q_8,$

but $\phi_{12} = A^3$ and as $b_1 = 0$ we have $P_1 = 0$. So

$$a_{12}A^3 = A^3Q_0 + a_{17}^2a_{18}A\phi_5^3 + a_{17}^2a_{18}A\left(A^2 + \phi_5^3\right) + a_{18}(a_{17}^2 + a_{18}^3)A^3,$$

so $Q_0 = a_{12} + a_{18}^4$.

7.1.10 Degree 8.

We have

$a_{11}\phi_{11} = P_8Q_0 + P_7Q_1 + P_6Q_2 + P_5Q_3 + P_4Q_4 + P_3Q_5 + P_2Q_6 + P_1Q_7 + P_0Q_8,$

which gives

$$a_{11}\phi_{11} = (P_0 + a_{17}^3)\phi_5^4.$$

But ϕ_5 does not divide ϕ_{11} so $a_{11} = 0$ et $P_0 = a_{17}^3$.

7.1.11 Conclusion.

We now have the following systems:

$$\begin{cases} \operatorname{tr}(c_1) = 0 \\ N(c_1) + \operatorname{tr}(d) = 0 \\ q_5(c_1, d) = 0 \\ q_4(c_1, d) = 0 \\ q_1(d) = q_1^3(c_1) + N(c_1)^2 \\ q_4(d, c_1) = N(c_1)q_1^2(c_1) \\ N(d) = N(c_1)^3 \end{cases}$$

and

$$a_{18} = q_1(c_1), a_{17} = N(c_1) = \operatorname{tr}(d).$$

Solving the system formed by the linear equations in $d, \rho(d), \rho^2(d)$, we obtain $d = c_1^3$. We also have $b_1 = 0$ as $b_1\rho\left(b_1\right)\rho^2\left(b_1\right) = 0$. Therefore

$$P = c_1\phi_5 + c_1^3,$$

and

$Q = \phi_5^4 + q_1(c_1)A^2 + N(c_1)A\phi_5 + q_1(c_1)^2\phi_5^2 + q_1(c_1)N(c_1)A + q_3(c_1)^2\phi_5 + a_{12} + q_1(c_1)^4,$

therefore

$f\left(x\right) = x^{20} + a_{18}x^{18} + a_{17}x^{17} + a_{16}x^{16} + a_{12}x^{12} + a_{18}a_{12}x^{10} + a_{17}a_{12}x^9 + a_8x^8 + \left(a_{18}^7 + a_{18}^4a_{17}^2 + a_{18}^3a_{12} + a_{18}a_{17}^4 + a_1\right.$

Putting $L\left(x\right) = x\left(x + c_1\right)\left(x + \rho\left(c_1\right)\right)\left(x + \rho^2\left(c_1\right)\right)$ we have that $\left(A + P\right)\left(A + \rho\left(P\right)\right)\left(A + \rho^2\left(P\right)\right)$ is the polynomial ϕ associated to $L\left(x\right)^3$ wich leads us to study the divisibility of f by $L\left(x\right)^3$. We have in our case $f = L\left(x\right)^3\left(L\left(x\right)^2 + a_{12}\right) + a_{16}x^{16} + a_8x^8 + a_4x^4 + a_2x^2 + a_1x + a_0$.

7.2 Case where P_2 divides ϕ.

We will write P for P_2 in this section in order to make the calculus more readable.

From theorem 7 we have

$$\phi = (\phi_5 + R)(A\phi_5 + Q)(A\phi_5 + \rho(Q))\left(A\phi_5 + \rho^2(Q)\right),$$

where R is a symmetrical polynomial of F_q of degree 1 and Q is a symmetrical polynomial of F_{q^3} of degree 4. We will denote $R = as_1 + b$ and $(A\phi_5 + Q)(A\phi_5 + \rho(Q))\left(A\phi_5 + \rho^2(Q)\right) = \sum_{i=0}^{15} Q_i$. We will identify degree by degree the expression of ϕ.

7.2.1 Degree 17.

We have

$$\phi_{20} = A^3\phi_5^4 = \phi_5 Q_{15},$$

so $Q_{15} = A^3\phi_5^3$.

7.2.2 Degree 16.

We have

$$a_{19}\phi_{19} = \phi_5 Q_{14} + as_1 Q_{15} = \phi_5 Q_{14} + as_1 A^3\phi_5^3,$$

which implies ϕ_5 divides ϕ_{19} but this is not the case hence $a_{19} = 0$ and $Q_{14} = as_1 A^3\phi_5^2$.

7.2.3 Degree 15.

We have

$$a_{18}\phi_{18} = \phi_5 Q_{13} + as_1 Q_{14} + bQ_{14} = \phi_5 Q_{13} + as_1^2 A^3\phi_5^2 + bA^3\phi_5^3,$$

which implies ϕ_5 divides ϕ_{18} but this is not the case hence $a_{18} = 0$ and $Q_{13} = A^3\left(a^2 s_1^2\phi_5 + b\phi_5^2\right)$.

7.2.4 Degree 14 and 13

We have

$$a_{17}\phi_{17} = \phi_5 Q_{12} + as_1 Q_{13} + bQ_{14}, \tag{2}$$

and

$$a_{16}\phi_{16} = 0 = \phi_5 Q_{11} + as_1 Q_{12} + bQ_{13} = \phi_5 Q_{11} + as_1 Q_{12} + bA^3\left(a^2 s_1^2\phi_5 + b\phi_5^2\right), \tag{3}$$

(2) implies that Q_{12} is divisible by ϕ_5 or $a = 0$. Lets assume $a \neq 0$. From (2) we have

$$a_{17}\frac{\phi_{17}}{\phi_5} = Q_{12} + a^3 s_1^3 A^3.$$

(we can show easily that ϕ_5 divides ϕ_{17} by calculus). As ϕ_5 divides Q_{12} it divides $a_{17}\frac{\phi_{17}}{\phi_5} + a^3 s_1^3 A^3$ too. But

$$a_{17}\frac{\phi_{17}}{\phi_5} + a^3 s_1^3 A^3 = a_{17} s_3^4 + R_1,$$

so $a_{17} = 0$. As ϕ_5 does not divide $s_1^3 A^3$ it means $a = 0$ and $Q_{12} = 0$. We now have, in both case

$$\phi = (\phi_5 + b)\left(\sum_{i=0}^{15} Q_i\right).$$

We know that $\phi_5 + b$ is irreducible if $b \neq 0$ ([11]), which is in contradiction with the fact that f is APN over infinitely many extension of F_q and then $b = 0$.

We now have $Q_{15} = A^3\phi_5^3, Q_{14} = Q_{13} = Q_{12} = Q_{11} = 0$.

7.2.5 Degree 12 to 8.

We have

$$a_{15}\phi_{15} = \phi_5 Q_{10},$$

as ϕ_5 does not divide ϕ_{15} we have $a_{15} = 0$ and $Q_{10} = 0$. The same method can be applied until the degree 8. It gives $a_{14} = a_{13} = a_{12} = a_{11} = 0$ and $Q_9 = Q_8 = Q_7 = Q_6 = 0$.

7.2.6 Degree 7.

We have

$$a_{10}\phi_{10} = a_{10}A\phi_5^2 = Q_5\phi_{10},$$

so $Q_5 = a_{10}A\phi_5$.

7.2.7 Degree 6.

The same argument than in section 7.2.5 gives $a_9 = 0$ and $Q_4 = 0$.

7.2.8 Degree 5.

We have

$$a_8\phi_8 = 0 = Q_3\phi_5,$$

therefore $Q_3 = 0$.

7.2.9 Degree 4 and 3.

The same argument than in section 7.2.5 gives $a_7 = a_6 = 0$ and $Q_2 = Q_1 = 0$.

7.2.10 Degree 2.

We have

$$a_5\phi_5 = Q_0\phi_5,$$

therefore $Q_0 = a_5$.

7.2.11 Conclusion.

In conclusion we have

$$\phi = \phi_5\left(A^3\phi_5^3 + a_{10}A\phi_5 + a_5\right) = \phi_{20} + a_{10}\phi_{10} + a_5\phi_5,$$

which gives $f(x) = x^{20} + a_{16}x^{16} + a_{10}x^{10} + a_8x^8 + a_5x^5 + a_4x^4 + a_2x^2 + a_1x + a_0$.